ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0035

Research on Standardization of Test Document Set Based on Automotive Penetration Test

Yanyan Han[1, a, *], Kexun He[1, b] and Wen Shao[1, c]

[1]CATARC Software Testing (Tianjin) Co., Ltd, Tianjin, 300300, China

[a]hanyanyan@catarc.ac.cn, [b]hekexun@catarc.ac.cn, [c]shaowen@catarc.ac.cn

Abstract

In recent years, automotive cyber security incidents occur frequently, WP 29 Passed R155, the world's first mandatory automotive cyber security regulation. No matter from the perspective of security enhancement or meeting the requirements of standards and regulations, enterprises need to carry out penetration testing in the process of research and development. However, including standards and regulations, there is no uniform acceptance specification for the deliverables of penetration testing. According to KBA's requirements for type approval, type approval needs to review test documents in the R&D process, so the quality of test documents becomes particularly important. This paper aims to study the specification of penetration test document set based on domestic and foreign regulations and standards, and help enterprises improve the quality of penetration test documents.

Keywords

Automotive; Penetration test; Test document set.

1. INTRODUCTION

In recent years, automotive cyber security incidents occur frequently. It is imperative to find and repair security vulnerabilities before the vehicle is put on the market. An effective way to identify security vulnerabilities is to perform security tests, such as penetration tests of target systems. Penetration test is usually black box test or gray box test, and the test effect depends largely on the experience and professional ability of the test engineer. OEM usually needs to establish a special team or carry out the test through a third-party laboratory. However, at present, there is no standardized method on how to conduct vehicle penetration testing, there is no unified acceptance specification for the deliverables of penetration testing, and the quality of test documents such as test reports is mixed.

January 22, 2021, WP 29 Passed R155, the world's first mandatory automotive cyber security regulation. R155 is the first mandatory vehicle cyber security regulation in the world, which requires vehicle models to obtain vehicle cyber security management system certification and vehicle cyber security type certification. In August of the same year, ISO officially released ISO/SAE 21434, which standardized the construction of the cyber security management system and the research and development of automotive product cyber security in the form of technical standards, and supported and guided vehicle manufacturers to implement R155 regulations. R155 requires OEMs to verify the effectiveness of the security measures implemented through appropriate and adequate testing [1]. The ISO/SAE 21434 standard provides the V model to guide the implementation of R&D process testing. Whether it is the integration verification process in the V model or the vehicle cyber security validation process, ISO/SAE 21434 mentions that penetration testing can be used [2]. However, neither of the two regulations put forward specific requirements for penetration testing, nor did they specify the documents to be delivered for penetration testing.

According to KBA's requirements for type approval, type approval needs to review test documents in the R&D process [3], so the quality of test documents becomes particularly important. This paper aims to study the specification of penetration test document set based on domestic and foreign regulations and standards, so as to help enterprises improve the quality of penetration test documents.

2. GENERAL REQUIREMENTS FOR PENETRATION TEST DOCUMENT SET

The test document set of penetration test mainly refers to all test documents that need to be sorted and prepared when conducting penetration test on test samples. The purpose is to verify whether the test samples meet the requirements of the test basis. This paper studies the specification of test document set from three levels.

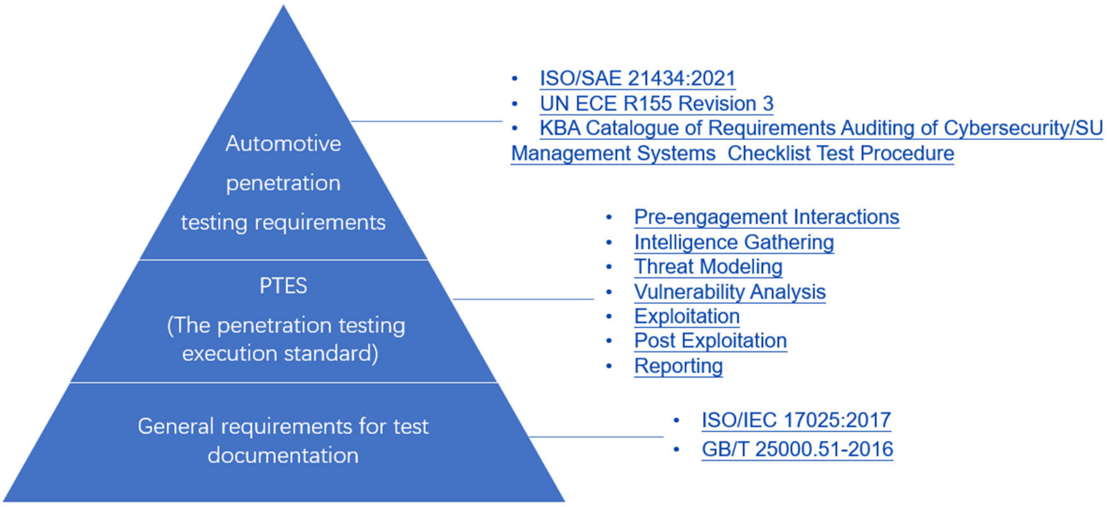
Automotive penetration testing requirements
ISO/SAE 21434:2021
UN ECE R155 Revision 3
KBA Catalogue of Requirements Auditing of Cybersecurity/SU Management Systems Checklist Test Procedure
PTES (The penetration testing execution standard)
Pre-engagement Interactions
Intelligence Gathering
Threat Modeling
Vulnerability Analysis
Exploitation
Post Exploitation
Reporting
General requirements for test documentation
ISO/IEC 17025:2017
GB/T 25000.51-2016

Figure 1. Three levels of requirements

The first level is to meet the general requirements of test documents. Mainly the requirements of consistency and traceability [4] [5].

The information contained in each document in the test document set shall be correct and verifiable.

The contents of all documents in the test document set shall be free of errors and ambiguities, and the information expressed shall be clearly described or can be verified by the existing technology. For example, each vulnerability should clearly describe the operation steps, input information, specific vulnerability information, etc. when the vulnerability is found, without error and ambiguity, so that it can be reproduced according to the description of the vulnerability.

Each document in the test document set shall not contradict itself.

Each document in the test document set shall include:

——Title;

——Product identification;

——Modification history, or any other element describing the evolution of the document;

——Contents or description of contents;

——Information about authors and reviewers;

——Description, clear identification, important parameters and state of test samples when necessary.

At the second level, penetration testing should be divided into seven stages by referring to the execution standard of penetration testing (PTES): pre-engagement Interactions, intelligence Gathering, threat Modeling, vulnerability Analysis, exploitation, post Exploitation and reporting [6].

The third level, according to the characteristics of vehicle penetration testing, in ISO/SAE 21434, it is required to carry out cyber security validation activities at the vehicle level, carry out penetration testing around cyber security goals, to find weaknesses in products, to prove the appropriateness and realization of cyber security goals related to threat scenarios and corresponding risks, and to quantify the scope and depth of penetration testing through CAL level. The vehicle penetration test process can be divided as follows:

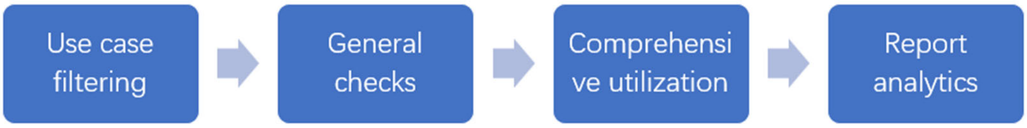

Figure 2. The vehicle penetration test process

(1) Use case filtering: select the test cases suitable for the cyber security goals and tested objects to be verified from the basic test case library.

(2) General checks: execute the adaptation case library obtained in step (1) to form the basic attack and vulnerability library.

(3) Comprehensive utilization: according to the test results in step (2) and the experience of penetration testers, carry out further testing and vulnerability utilization.

(4) Report analysis: prepare a test report, at least including vulnerability description, threat type, test steps and repair plan.

Correspondingly, the penetration test document set generally includes test plans, test cases, test reports, etc. It can be composed of one document or multiple documents.

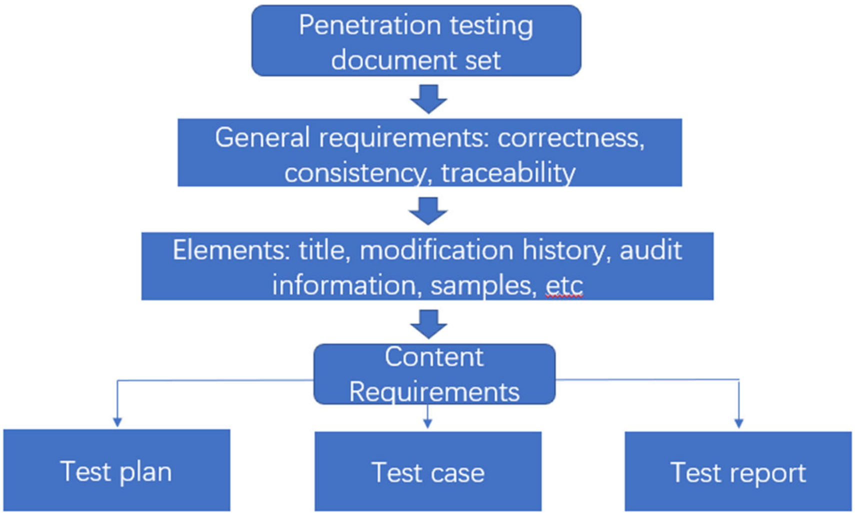
Penetration testing document set
General requirements: correctness, consistency, traceability
Elements: title, modification history, audit information, samples, etc
Content Requirements
Test plan
Test case
Test report

Figure 3. Composition of penetration test document set

3. CONTENT REQUIREMENTS OF PENETRATION TEST DOCUMENT SET

3.1. Test Plan Requirements

The test plan shall determine the scope and objectives of the penetration test, such as the cyber security goals to be verified.

The test plan shall determine the basis for judging the test results. For example, it is necessary to determine the evaluation methods of security vulnerability hazard level and product security level.

The test plan shall specify the environmental requirements for the test.

The test plan shall be formulated to specify the progress of each test activity and test milestone. Test activities may include: test environment construction, test documentation, test execution, etc.

The test plan shall identify, update and record the risks existing in the test activities, and provide countermeasures.

The test plan shall specify the personnel required for each test activity.

The test plan shall specify the equipment or tools required for the implementation of test activities. The equipment shall be traceable and need to be calibrated when applicable.

3.2. Test Case Requirements

When designing test cases, test coverage shall be evaluated to determine the adequacy of test activities.

The description of each test case shall include:

——Test objectives;

——Unique identifier;

——Test conditions;

——Test input;

——Detailed implementation steps;

——Expected results of test cases

——Criteria for interpretation of results.

The test case should also identify the corresponding relationship with the cyber security goals.

3.3. Test Report Requirements

The test report shall include all summaries of test case results.

The test report shall verify that all test cases have been executed according to the test plan.

For each test case, the test report shall include the following contents:

——Identifier of test case;

——Test execution date;

——Personnel performing the test;

——Results of test case execution;

——Vulnerability information found.

4. CONCLUSION

Whether from the perspective of safety improvement or meeting the requirements of standards and regulations, penetration testing is required in the process of automotive research and development. However, including standards and regulations, there is no uniform acceptance specification for the deliverables of automotive penetration testing. According to KBA's requirements for type approval, type approval needs to review test documents in the R&D process, so the quality of test documents becomes particularly important. Based on domestic and foreign regulations and standards, this paper studies the specification of penetration test document set, and puts forward specific specification requirements from the general requirements and content requirements, so as to provide enterprises with reference to improve the quality of penetration test documents.

ACKNOWLEDGMENTS

This paper was supported by the subject “Research on automotive cyber security detection method for international certification and domestic supervision”.

REFERENCES

[1] E/ECE/TRANS/505/Rev.3/Add.154, (2021). UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. https://unece.org/sites/default/files/2021-03/R155e.pdf.

[2] ISO/TC 22/SC 32 Electrical and electronic components and general system aspects, (2021). ISO/SAE 21434:2021(E) Road vehicles — Cybersecurity engineering.

[3] Kraftfahrt-Bundesamt, (2021). Application of the Rules for designation/recognition for technical services (categories A, B, D) for testing in the context of the KBA-type approval procedure according to UN-R 155/156. https://www.kba.de/EN/Themen_en/Typgenehmigung_en/Zum_Herunterladen_en/BenennungTechnischerDienste_en/anwendung_Regeln_TD_R155_R156_en.pdf?__blob=publicationFile&v=3

[4] GB/T 25000.51—2016 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Part 51: Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing, China Standards Press

[5] ISO/IEC 17025: 2017 General requirements for the competence of testing and calibration laboratories.

[6] Information on http://www.pentest-standard.org/index.php/Main_Page